

## **REMARKS**

Applicant hereby responds to the Office Action mailed on November 17, 2003. In the Office Action, the Examiner rejects all pending claims in the application (Claims 1-38).

As will be set forth in greater detail below, Applicants respectfully submit that the pending claims, along with the amended claims herein described below, are patentable over all the prior art of record. Accordingly, reconsideration of the application in light of the following remarks and amended claims is respectfully requested.

### ***35 U.S.C. § 112 Rejections***

#### **Claims 1-5 and 12-26**

Claims 1-5 and 12-26 stand rejected under 35 U.S.C. § 112, first paragraph, as being unpatentable for failing to comply with the enablement requirement. The Examiner contends that the subject matter was not described in the specification in such a way as to enable one skilled in the art to which it pertains, or with which it is most nearly connected, to make and/or use the invention. Applicants respectfully traverse this rejection.

More specifically, the Examiner contends that “said forms comprising said security processor authorization” found in Claims 1, 12, 17, and 22, to one of ordinary skill, means the authorization is present in the form and that this feature is not supported by the specification. Applicants respectfully traverse this rejection. Applicants respectfully submit that the feature is supported in the specification. For example, the specification describes the components on page 9, lines 30-34;

...virtual point of sale (POS) gateway processor 190 which is in the financial authorization entity secure processor 170. Also in the secure processor 170, and coupled to POS gateway processor 190, is payment authorization gateway 180. Further, wallet server 140 is coupled to merchant server 130 and to virtual point of sale (VPOS) gateway processor 190.

Moreover, on page 10, lines 31-34, and page 11, line 1, the specification describes the process;

Virtual gateway 190 queries payment authorization gateway 180 to obtain authorization for the payment. Upon obtaining such authorization, virtual POS gateway transmits the information to

wallet server 140. Wallet server 140 then completes an authorization form and transmits the form to merchant server 130.

As described above, authorization is obtained via virtual gateway 190 and through authorization gateway 180. The authorization is then transmitted to wallet server 140 wherein the authorization forms are completed with security processor authorization and sent on to merchant server 130. Therefore, we respectfully submit that the authorization is present within the form, as the Examiner suggests, and that it is adequately supported by the specification.

For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claims 1, 12, 17, and 22 and the Claims dependant thereto; 2-5, 13-16, 18-21, and 23-26 under 35 U.S.C. § 112, first paragraph.

#### **Claims 1-5 and 12-28**

Claims 1-5 and 12-28 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention. More specifically, the Examiner contends that in Claims 1, 12, 17, and 22, which recite the limitation "said security processor authorization" in sections 1e, 12e, 17e and 22e, that there is insufficient antecedent basis for this limitation in the claim. Upon entry of the foregoing amendments, Applicants eliminate the antecedent basis concern by amending part e of Claims 1, 12, 17, and 22 to read:

e. assembling forms for the transaction, said forms comprising an authorization by said security processor ~~authorization~~ of said input to said security processor;

The Examiner next states that Claims 28 and 36 which recite the limitation "instrument" in line 2, has an insufficient antecedent basis for this limitation in the claim. Upon entry of the foregoing amendments, Applicants eliminate the antecedent basis concern by amending Claims 28 and 36 to read:

28. The transaction system of Claim 27, further operative to provide said validation for different combinations of said instruments and security processors.

36. The transaction system of Claim 35, further operative to

provide said validation for different combinations of said instruments and security processors.

The Examiner next states that an insufficient antecedent basis is present in Claim 2, line 3 wherein Claim 2 recites "said merchant." Upon entry of the foregoing amendments, Applicants eliminate the antecedent basis concern by amending Claim 2 to read:

2. The method of Claim 1 further directed to providing such transaction validation for different combinations of instruments and security processors without requiring changes to transaction processing by said a merchant.

These amendments should now exhibit a proper antecedent basis for these limitations in the Claims. For the amendments made above, Applicants respectfully request that the Examiner withdraw the rejection of Claims 1-5 and 12-38 under 35 U.S.C. § 112.

#### **Claims 1-6 and 12-16**

Claims 1 and 12 stand rejected under 35 U.S.C. § 112, second paragraph, as being unpatentable for including a relative term which renders the Claims indefinite. The Examiner contends that the term "incident" in Claims 1(f) and 12(f) is not defined by the Claim, that the specification does not provide a standard for ascertaining the requisite degree, and that one of ordinary skill in the art would not be reasonably apprised of the scope of the invention. Upon entry of the foregoing amendments, Applicants eliminate the indefiniteness concern by deleting "incident" from Claims 1(f) and 12(f). This amendment should render the Claims definite. Moreover, since Claims 2-6 and Claims 13-16 depend respectively therefrom, they should now be rendered definite as well.

#### **Claims 27-38**

Claims 27, 31, and 35 also stand rejected under 35 U.S.C. § 112, second paragraph, as being unpatentable for including a relative term which renders the Claims indefinite. The Claims recite an interface, "operative to permit validation of said form." The Examiner suggests that the

interface does not receive the form.

The interface merely provides, for example, a third party conduit with which to be able to permit validation of the form, by the merchant, from the credit supplier. In order to validate the form, the interface does not necessarily need to have received the form, as adequately disclosed in the specification on page 11, lines 2 - 9. The merchant communicates with a third party, which in turn communicates back to the credit supplier to double check the information on the form received by the merchant, to validate the form. Moreover, page 11, line 7 of the specification refers to, "authenticating the completed form." If the process were as the Examiner suggests, then the line in the specification would preferably read, "completing the authenticating form," which would suggest that the interface (third party) had received the form such that they needed to add something to make it complete. Further support exists on page 11, lines 20-26, where the specification discusses how the merchant server **queries** (emphasis added) the security server (via the interface) for credit supplier authentication of the authorization form (this embodiment does not include forwarding, transmitting, or sending any form). Page 11, lines 23-25 also discusses how the credit supplier authenticates the authorization form based on the information from the Smart Card and transmits an authentication to the merchant without returning any previously received authentication form.

For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claims 27, 31 and 35 and the Claims dependant thereto; 28-30, 32-34, and 36-38 under 35 U.S.C. § 112, second paragraph.

### ***35 U.S.C. § 102(e) Rejections***

#### **Claims 1-5, 12 -26 and 27-38**

Claims 1-5, 12-26, and 27-38 are rejected under 35 U.S.C. § 102(e) as being clearly anticipated by Daly et al. (Daly), U.S. Patent No. 5,878,141. Applicants respectfully traverse the rejection. More specifically, the Examiner contends that Daly teaches each step of the independent claims 1 and 12, and the claims that depend there from.

The Examiner cites step, "validating the transaction with the second authorization (column 8, lines 47-61)"; however, this step in Daly is inconsistent with the process described by

the presently claimed invention. The Daly reference discusses a second authorization by the purchaser. Column 8, lines 49-53 of the Daly reference reads;

If the purchaser confirms (second authorization) the purchase transaction, the processing unit attaches an unforgeable digital signature on behalf of the purchaser to authorize the purchase and to validate for the merchant that a sale has been consummated.  
(emphasis added)

This is contrary to the second authorization discussed in the presently claimed invention. The second authorization of the presently claimed invention includes a process wherein the credit supplier is twice queried through a security processor to verify the authorization, not the purchaser. Claims 1(g) and 12(h) from the presently claimed invention recite, "validating said transaction with said second authorization of said forms received from said security processor." Wherein, as set forth in the specification and shown in Figure 1, the security processor includes; a credit supplier coupled to a payment authorization gateway and the authorization gateway is coupled to a virtual POS gateway.

In Daly, the reference is directed towards verifying that the merchant and purchaser share in at least one common credit supplier to carry out the transaction and whether the purchaser has the available credit or account funds available to cover the amount of the transaction. Daly does not include the claimed step as recited above.

In the presently claimed invention, a purchaser may use their smart card to secure payment for goods or services from a credit supplier through the secure wallet (authorization) server, the credit supplier sends the authorization for payment back to the wallet server that in turn prepares the forms and sends the forms on to the merchant. The merchant, directly or through a third party, queries back to the credit supplier asking if it indeed did authorize the purchase. If so, the authorization form is completed via the wallet server interface for the merchant and the sale is completed.

The Examiner also asserts that the statement, "authorizing the forms twice at a security processor" in the Daly reference (column 7, lines 5-17; column 8, lines 20-61) is relevant to the presently claimed invention. Again, the Daly reference describes a different process than the presently claimed invention and it does not describe authorizing forms twice by a security processor. The Daly reference is directed towards verifying that the merchant and purchaser

share in at least one common credit supplier to carry out the transaction and whether the purchaser has the available credit or account funds available to cover the amount of the transaction.

In contrast, the presently claimed invention does not authorize the forms twice at a security processor, but authorizes the forms twice by a security processor. In other words, the security processor does not receive the forms. The form is first assembled once the wallet server receives an initial authorization from the security processor. The form is then transmitted to the merchant who in turn verifies that the security processor did indeed authorize the transaction, but does not transmit the form to the security processor to accomplish this, as described at page 11, lines 16-28 of the present invention. This structured form movement is important because the less movement of verification forms, the less risk there is of fraudulent activity to occur, i.e. there are fewer transmissions that might be intercepted, fewer in roads for hackers or fraudulent purchasers, and fewer items to be encrypted and decrypted. In the present invention, the forms are transferred only once, from the authorization server to the merchant. This process has the benefit of twice authorizing a purchase, yet only transmitting the forms one time.

As such, the Daly reference does not include, "providing said forms to said transaction and sending a request to said security processor for a second authorization of said forms;" nor "validating said transaction with said second authorization of said forms received from said security processor," as is required by independent Claim 1.

The Daly reference also does not include, "said merchant processing said forms and sending a request to said security processor for a second authorization of said forms;" nor "validating said transaction with said second authorization of said forms received from said security processor," as is required by independent Claim 12.

For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claims 1 and 12 and the Claims dependant thereto; 2-5 and 13-26 under 35 U.S.C. § 102(e).

#### **Claims 27-38**

Claims 27-38 are rejected under 35 U.S.C. § 102(e) as being clearly anticipated by Gifford, U.S. Patent No. 6,049,785. Applicants respectfully traverse the rejection. More

specifically, the Examiner contends that Gifford teaches each step of the independent claims 27, 31, and 35 and the claims that depend there from.

The Examiner states that the presently claimed invention is anticipated by the following disclosure of Gifford:

a security server receives the data from the authorization server and generates and transmits an authorization form to said authorization server, and an interface coupled to the security server and operative to permit validation of said form and complete a secure online virtual transaction (column 8, lines 47-61)

Again, referencing arguments contained herein above, the security server of the presently claimed invention does not generate or assemble the authorization form. In the presently claimed invention, it is the wallet (authorization) server that assembles the authorization form and forwards it to the merchant. Moreover, the presently claimed invention provides for a second verification of the authorization by having the merchant query the security server. This process is important because it allows for a two way independent verification system and helps deter fraudulent actions. The two independent verification system includes, the buyer via the wallet (authorization) server obtaining authorization for his purchase and the merchant verifying the buyers authorization with the credit supplier.

As such, Gifford does not include;

said security server coupled to receive said input from said authorization server and operative to generate and transmit an authorization to said authorization server;

said authorization server coupled to receive said authorization from said security server and operative to generate and transmit an authorization form; and

an interface coupled to said security server and operative to permit validation of said form and complete a secure on-line virtual transaction with said user.

which is required by independent Claim 35 and similarly required by independent Claims 27 and 31.

In contrast, the Gifford reference uses a completely different method to verify authorization. Specifically, the Gifford reference verifies authorization by the merchant

verifying that a payment order was not previously used. The merchant checks for previous use through, "a payment computer or maintaining a merchant computer database of previously accepted payment orders. (column 7, lines 59-61)" As such, the Gifford reference does not disclose querying the security server for verification. Also, see generally, Gifford column 7, lines 51-61 and column 8, lines 51-64.

For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claims 27, 31, and 35 and the Claims dependant thereto; 28-30, 32-34 and 36-38 under 35 U.S.C. § 102(e).

#### **Claims 6 and 8-11**

Claims 6 and 8-11 are rejected under 35 U.S.C. § 102(e) as being clearly anticipated by Gifford, U.S. Patent No. 6,049,785. Applicants respectfully traverse the rejection. More specifically, the Examiner contends that Gifford teaches each step of independent claim 6 and claims 8-11 that depend there from.

As previously discussed, the presently claimed invention provides for a second verification of the authorization by having the merchant query the security server. In contrast, the Gifford reference uses a different method to verify authorization, namely, by the merchant verifying that a payment order was not previously used. The Gifford merchant checks for previous use through, "a payment computer or maintaining a merchant computer database of previously accepted payment orders." (column 7, lines 59-61) Gifford does not query the security server for verification. Also, to clarify function, the Gifford payment computer is not equivalent to the security server or credit supplier of our invention as it pertains to any re-verification. The Gifford payment computer may act in a closer way to the presently claimed wallet server, as seen by a comparison of Gifford Figure 13 to the present Figure 1.

The Gifford reference does not include from Claim 6 of the presently claimed invention, "said merchant querying said credit provider for authentication of said credit provider response;" nor "completing said virtual transaction using authorization from said credit provider."

For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claim 6 and the Claims dependant thereto; 8-11 under 35 U.S.C. § 102(e).



### *35 U.S.C. § 103(a) Rejections*

#### **Claim 7**

Claim 7 is rejected under 35 U.S.C. § 103(a) as being unpatentable over Gifford, U.S. Patent No. 6,049,785. The Examiner claims Gifford teaches the use of a smart card. More specifically, that it would have been obvious to open a wallet and input a smart card in order to authenticate a transaction. Applicants respectfully traverse the rejection.

It may be well known in the art to use smart cards. It may also be well known to one skilled in the art to use a smart card in the context of an electronic wallet similar to using a regular credit card as an input to an electronic wallet. However, contrary to the Examiner's statements, the presently claimed invention goes way beyond simple use of a transaction card with an electronic wallet. For example, the use of the smart card in the context of the present invention provides greater security for an on line purchasing system.

The presently claimed invention allows a merchant to securely interact with purchasers without having merchants initiate changes to accommodate each different smart card or wallet. The presently claimed invention lets the merchant receive the forms from a purchase authorization, prepared by the wallet server. Next, the merchant verifies the information a second time with the credit supplier. In this fashion, the merchant is assured of secured transactions without having to retrofit each new smart card or similar technology. Furthermore, the merchant has peace of mind against fraud because the transaction is channeled through a wallet server, requiring a smart card for authorization. The merchant then is able to double check the authorization a second time, verifying the transaction.

Gifford, however, uses a less secure authorization process, see Gifford's Figure 6. In Gifford, the buyer directly contacts the credit supplier, instead of through an authorization server as in the presently claimed invention, to obtain a preauthorized payment order. The Gifford buyer then uses the payment order to forward to the merchant for payment. The merchant in Gifford is in a much less secure position than those using the presently claimed invention. The Gifford merchant must rely on a supposed encrypted, preauthorized payment order directly from the buyer. In the presently claimed invention, the financial matters of the transaction are carried out and verified by third parties and the wallet (authorization) server, which is a much more

secure method than a merchant and buyer dealing directly with each other, regardless of the supposed greater security measures by utilizing a smartcard.

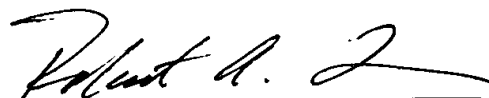
For the reasons set forth above, Applicants respectfully request that the Examiner withdraw the rejection of Claim 7 under 35 U.S.C. § 103(a).

### CONCLUSION

In view of the foregoing, Applicants respectfully submit that all of the pending and amended claims are allowable over the prior art of record. Reconsideration of the application and allowance of all pending and amended claims (1- 38) are earnestly solicited. Should the Examiner wish to discuss any of the above in greater detail or deem that further amendments should be made to improve the form of the claims, the Examiner is invited to telephone the undersigned at the Examiner's convenience.

Dated: February 17, 2004

Respectfully submitted,

By:   
Robert A. Iussa  
Reg. No. 51,337

**SNELL & WILMER L.L.P.**  
400 East Van Buren  
One Arizona Center  
Phoenix, Arizona 85004-2202  
Telephone: (602) 382-6226  
Facsimile: (602) 382-6070